AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No.	MJ18-496
HP Spectre Laptop, as further described in Attachment A		

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

HP Spectre Laptop, as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 371, 1073, 1343, 1546	Conspiracy to Defraud the United States, Unlawful Flight from Prosecution, Wire Fraud, Visa Fraud

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT RICHARD LIN, U.S. STATE DEPT

Printed name and title

Sworn to before me pursuant to Local Criminal Rule 4.1.

Date: October 26, 2018

Judge's signature

City and state: SEATTLE, WASHINGTON

MARY ALICE THEILER, U.S. MAGISTRATE JUDGE

Printed name and title

2016R00055

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, RICHARD LIN, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of a digital device, hereinafter the "SUBJECT DEVICE," which is currently in law enforcement possession, and the extraction from that device of electronically stored information described in Attachment B.

2. I am a Special Agent of the Diplomatic Security Service (DSS), which is an agency of the United States State Department, and I have been so employed for over 15 years. I am presently assigned to the Document and Benefit Fraud Task Force at the United States Department of Homeland Security (DHS). This task force investigates sophisticated immigration frauds. In the context of my work for this task force, I have received and continue to receive specialized training and instruction from State Department officers who issue entry visas to foreigners overseas and DHS officers who issue employment documents to foreigners already inside of the United States. I am empowered under 22 U.S.C. § 2709 to investigate visa frauds, as well as to apply for and serve federal arrest and search warrants. My previous assignments include postings in New York, Washington, D.C., Los Angeles, Karachi, Pakistan, and Beirut, Lebanon, as well as numerous long-term temporary-duty assignments throughout the Middle East and South Central Asia. Prior to DSS, I served in the U.S. Marine Corps Reserve. I also have a Master's Degree in Public Administration from the University of Georgia.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1956 (Laundering of Monetary Instruments), Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, Section 1073 (Flight to Avoid Prosecution), Title 18, United States Code, Section 1546 (Visa Fraud), and Title 18, United States Code, Section 371 (Conspiracy) will be found on the SUBJECT DEVICE.

IDENTIFICATION OF THE SUBJECT DEVICE TO BE EXAMINED

5. The SUBJECT DEVICE is a black Hewlett Packard Spectre laptop bearing serial number 5CD74295HB.

STATEMENT OF PROBABLE CAUSE

6. Since in or about 2015, the United States Department of State has investigated PRADYUMNA K. SAMAL ("SAMAL") for submitting false and fraudulent applications for nonimmigrant workers to the United States Citizenship and Immigration Services ("USCIS"). During and in relation to that investigation, the Government recently applied for and obtained warrants authorizing searches of phones seized from SAMAL at the time of his arrest. The Affidavit submitted in support of that earlier Application is attached hereto as Exhibit A and incorporated as if fully set forth herein. As set out in Exhibit A: (1) SAMAL's companies filed over one hundred (100) petitions with USCIS that containing forged and false materials[1]; (2) law-enforcement agents

[1] Under Section 101(a)(15)(H) of the Immigration and Nationality Act ("INA"), U.S.-based employers can petition for foreign nationals to enter the United States and work under specialty occupations.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

searched SAMAL's companies' offices on or about October 5, 2017 and thereafter approached two of SAMAL's co-conspirators in or around January 2018; (3) in or around February 2018, SAMAL sold the parts of his businesses that were under investigation; (4) in or around February 2018, SAMAL fled to India to avoid prosecution; and (5) on or about August 28, 2018, SAMAL returned to the United States, where he was arrested upon his arrival pursuant to an under seal warrant issued by the Honorable Mary Alice Theiler, United States Magistrate Judge.

7. In the paragraphs below, I set forth additional facts that the Government has discovered since the Affidavit (Exhibit A) was filed. As a preliminary matter, however, I respectfully submit that the facts set out in Exhibit A themselves establish probable cause that the SUBJECT DEVICE will contain evidence of the crimes of Unlawful Flight from Prosecution, Visa Fraud, and Conspiracy.

A. Probable Cause the SUBJECT DEVICE Will Contain Evidence of Unlawful Flight from Prosecution, Visa Fraud, and Conspiracy

8. As with his phones, SAMAL traveled from India to the United States with the SUBJECT DEVICE. Thus, for the reasons set out in Exhibit A, the SUBJECT DEVICE will contain evidence of the crimes of unlawful flight from prosecution, visa fraud, and conspiracy. Specifically, there is probable cause to believe that the SUBJECT DEVICE will contain evidence of SAMAL's whereabouts (e.g., geolocation information, records of wireless networks to which he was connected) while he was out of the United States and his business activities (e.g., documents he helped create, and his email correspondence). This information not only may tend to establish whether SAMAL left the United States to evade prosecution, but also whether he did so because of his consciousness of guilt for the crimes of visa fraud and conspiracy.

9. Moreover, since filing the Affidavit to search SAMAL's phones, the Government has continued to develop evidence that establishes additional probable cause that the SUBJECT DEVICE will contain evidence of the crimes of unlawful flight from prosecution, visa fraud, and conspiracy. Specifically:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. **Documents on SAMAL's phone:** Investigators found documents on SAMAL's phone that appear to evidence his intent to flee from prosecution and his consciousness of guilt for the crimes of visa fraud and conspiracy to commit visa fraud. In one WhatsApp chat found on SAMAL's phone, SAMAL sent one of his employees in India several photographs of office space under construction and India-based employees at their workstations. SAMAL's phones also contained a screenshot of a letter SAMAL received from Burger King India regarding a Term Sheet SAMAL had entered into with to open a chain of fast-food restaurants in India and his purported breach of that Term Sheet. Further, SAMAL's phone contained invoices, purchase orders, photographs, and chats regarding the renovation (and potential purchase) of a home in India. These transactions appear to show SAMAL's efforts to establish a more permanent business and residence in India, thus relocating the focus of his work and life away from the United States while under investigation. In my training and experience, the actual contracts relevant to these various transactions – i.e., to expand business space, franchise fast-food restaurants, and renovate/purchase a residence – are likely to be find on SAMAL's computing device.

b. **Witness Interviews**: Since SAMAL returned to the United States, investigators have also interviewed witnesses who stated that they communicated with SAMAL while he was overseas. During those interviews, the witnesses referred to written correspondence they exchanged with SAMAL, which there is probable cause to believe will be found on the SUBJECT DEVICE because it was SAMAL's personal computing device while overseas:

i. On September 24, 2018, I interviewed an individual referred to herein as WITNESS A, who served as a Chief Financial Officer at Divensi and Azimetry until in or around December 2017.[2] WITNESS A told me that he corresponded with SAMAL about SAMAL's absence from the United States over the telephone, and that he corresponded with SAMAL over email about the operation of the business, while SAMAL was overseas. WITNESS A stated that SAMAL told him/her over the telephone that he was in India because of the Government's investigation into him.

ii. During an interview on October 10, 2018, an individual referred to herein as WITNESS B, who served as a Chief Technology Officer at Divensi between in or around March 2017 and in or around July 2018, said that he communicated with SAMAL about SAMAL's plans (if any) to return to the United States. WITNESS B told me that SAMAL told him/her that SAMAL was staying out of the United States in

---

[2] WITNESS A has a prior conviction for Bank Fraud in the Western District of Washington. WITNESS A has also been investigated by the Government for engaging in the acts of visa fraud for which SAMAL has been under investigation. WITNESS A signed at least four of the petitions in which Azimetry falsely claimed that the foreign nationals named in the petitions had been earmarked to work on projects for a client named in the petitions.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

part because he believed it would help him improve his negotiating position with the Government regarding a "fine" that the Government could impose against his businesses for labor-law violations. One WhatsApp online-messaging chat that investigators found on SAMAL's phone between WITNESS B and SAMAL appears to confirm that these discussions regarding the reasons for SAMAL's stay in India took place between the two individuals; in the chat, SAMAL told WITNESS B that he was preoccupied in India with visiting his ailing mother. WITNESS B told me that his email communications with SAMAL, as well as his telephone conversations with SAMAL during the same time period, gave him concern that SAMAL was not being honest with him about the reasons why SAMAL had left the United States for India.

iii. During an interview on October 10, 2018, an individual referred to herein as WITNESS C, who managed sales for SAMAL's business operations, told me that he visited SAMAL in India in August 2018. WITNESS C told me that, when he confronted SAMAL about the development of a new residence in India, SAMAL claimed that it was customary for Indian ex-patriates to purchase residences in India. WITNESS C told me that he exchanged emails with SAMAL about the businesses while SAMAL was in India. WITNESS C also told me that SAMAL told WITNESS C that SAMAL was the subject of a U.S. government investigation that could result in the issuance of a fine against SAMAL.

B. Probable Cause that the SUBJECT DEVICE Will Contain Evidence of Wire Fraud

10. There is also probable cause to believe that the SUBJECT DEVICE will contain evidence of two separate wire-fraud schemes that are presently under investigation.

11. ***First***, after SAMAL's arrest on August 28, 2018, I learned that SAMAL, his wife, and his companies (among others) recently were named as defendants in a civil lawsuit filed by Synapse, the company that purchased SAMAL's companies' H-1B-related operations in February 2018. In the lawsuit, Synapse alleges that SAMAL did not transfer all of the relevant information for client accounts that Synapse purchased (and performed services for), which caused SAMAL to continue to receive payments for work

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that was being performed by Synapse.[3] Specifically, Synapse alleges that SAMAL and his companies failed to provide Synapse with the bank account information and "client portal" logins that SAMAL's companies had used to interact with the client accounts that Synapse purchased. According to Synapse, "[b]y withholding access to the portals, [SAMAL] continues to receive funds from [Synapse's] customers for services provided by [Synapse] and which rightfully belong to [Synapse]." A chart produced to the Government by Synapse lists numerous clients, including Microsoft, as those whose payments SAMAL fraudulently diverted to his own use.

12. Bank records appear to show that SAMAL received payments from Microsoft for services performed by Synapse, concealed those payments using his personal accounts, and then transferred the bulk of those payments to an account in India in his own name. The byline on the international transfers referred to "Home Improvement," which appears to suggest that SAMAL used the ill-gotten gains to finance the home renovation described above.

13. More specifically, the chart below shows payments that Microsoft made to an account (referred to below as the "7364 account") held by Divensi Technology Inc. – a company that SAMAL purported to have sold to Synapse, thereby transferring to Synapse the right to perform services for Divensi Technology Inc.'s clients (and to receive payment for those services). SAMAL appeared to misappropriate payments made by Microsoft in exchange for those services performed by Synapse, contrary to his agreement with Synapse.

Transfer Into 7364 account	Corresponding Transfer Out of 7364 account
Mar. 20, 2018 $101,337.86 transfer from Microsoft to 7364 account	Mar. 20, 2018 $101,345.00 transfer to 7599 account (held by Alonzi Ventures, LLC)[4]

[3] Synapse's specific allegations are set out in a civil complaint against Samal and others that is now pending in King County Superior Court under the caption *Synapse Technologies LLC, et al. v. Azimetry Inc, et al.*, Case No. 18-2-20495-0 SEA.

[4] On the same day that it received the $101,345.00 transfer, the 7599 account transferred $65,000.00 to an account held by Sagarika Samal. The account held by Sagarika Samal proceeded to transfer the funds (on the same day) to SAMAL's account in India.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Mar. 22, 2018 $7,521.50 transfer from Microsoft to 7364 account	Mar. 22, 2018 $7,500.00 transfer to 9107 account (held by PK and Sagarika Samal)[5]
April 11, 2018 $60,865.90 transfer from Microsoft to 7364 account	April 11, 2018 $60,800.00 transfer to 9107 account (held by PK and Sagarika Samal)[6]
April 12, 2018 $6,036.80 transfer from Microsoft to 7364 account	April 12, 2018 $6,000.00 transfer to 9107 account (held by PK and Sagarika Samal)[7]
April 13, 2018 $6,624.80 transfer from Microsoft to 7364 account	April 13, 2018 $6,700.00 transfer to 9107 account (held by PK and Sagarika Samal)[8]
April 20, 2018 $6,528.76 transfer from Microsoft to 7364 account	April 20, 2018 $6,500.00 transfer to 9107 account (held by PK and Sagarika Samal)
April 30, 2018 $6,320.00 transfer from Microsoft to 7364 account	April 30, 2018 $6,300.00 transfer to 9107 account (held by PK and Sagarika Samal)

14. Of the funds referred to in the chart above, SAMAL appeared to direct that a significant percentage of them be transferred to an Indian bank account in his name. The chart below shows transfers from accounts owned by SAMAL's wife (Sagarika Samal) alone or jointly with SAMAL to an account in SAMAL's name at ICICI Bank in India. As the chart shows (and as described in additional detail in footnotes 4-8 above), almost all of the payments from Microsoft that SAMAL was required to send to Synapse appeared to be diverted to accounts in India.[9]

Origination Account	**Destination Account**	**Amount Transferred (and Contents of Memo. Line)**	**Date of Transfer**
Sagarika Samal, JP Morgan Chase (0147)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$50,000 (Home Improvement/Family Expenses)	Feb. 21, 2018
Sagarika Samal, JP Morgan Chase (0147)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$50,000 (Home Improvement/Family Expenses)	March 20, 2018
Sagarika Samal, JP Morgan Chase (0147)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$20,000 (Home Improvement/Family Expenses)	March 21, 2018

[5] On the same day as this transfer, the 9107 account transferred $8,000 to SAMAL's account in India.
[6] On the same day as this transfer, the 9107 account transferred $60,000 to Sagarika Samal's account with JP Morgan Chase (the "0147 account"). The 0147 account then transferred $35,000 to SAMAL's account in India, $19,800.00 to the 7599 account, and $4,000 to an account held by a separate SAMAL-owned entity named Airometric, Inc. (the "2603 account"). Both the 7599 account and the 2603 account proceeded to transfer the funds to Azimetry, Inc.'s account, which used the funds for business expenses.
[7] On the same day as this transfer, the 9107 account transferred $4,000 to the 0147 account and $2,000 to a separate account held by PK and Sagarika Samal. The 0147 account eventually transferred the funds to India.
[8] On the same day as this transfer, the 9107 account transferred $7,000 to the 0147 account, which aggregated it with the prior day's transfer (described in fn. 7 above) and sent $10,000 to SAMAL's account in India.
[9] The transfers to India did not represent a dollar-for-dollar diversion of payments from Microsoft, as some of the funds did not originate with Microsoft and some of the Microsoft funds did not end up in India.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Sagarika Samal, JP Morgan Chase (0147)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$35,000 (Home Improvement/Family Expenses)	April 11, 2018
Sagarika Samal, JP Morgan Chase (0147)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$10,000 (Home Improvement/Family Expenses)	April 13, 2018
P.K. & Sagarika Samal, JP Morgan Chase (9107)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$8,000 (Home Improvement/Family Expenses)	March 22, 2018
P.K. & Sagarika Samal, JP Morgan Chase (9107)	P.K. Samal, Icici Bank Ltd., Mumbai, India,	$8,000 (Home Improvement/Family Expenses)	April 30, 2018

15. There is probable cause to believe that evidence of SAMAL's diversion of funds owed to Synapse will be found on the SUBJECT DEVICE. Specifically, evidence of SAMAL's involvement in those transfers will be found on the devices he used to effective the transfers. In my training and experience, in order to conduct financial transfers from overseas, an individual like SAMAL typically would use an online banking portal from a personal computer, leaving records of that access behind.

16. ***Second***, after SAMAL's arrest on August 28, 2018, I received an email from a former employee of Divensi's referred to herein as VICTIM A. VICTIM A informed me that he/she worked at Divensi from April 2017 until its sale in February 2018, after which he/she became a Synapse employee. VICTIM A claimed that he/she made contributions to an employee-sponsored 401k plan during his employment, and instructed Divensi's accounting staff about the percentage of each paycheck to withhold and send to the 401k plan administrator. VICTIM A claimed that, following the February 2018 sale of certain aspects of SAMAL's businesses to Synapse, VICTIM A reached out to the 401k plan administrator to find out whether he could access his contributions. VICTIM A claimed that he/she learned that Divensi had failed to make contributions to his/her 401k plan.

17. VICTIM A also produced an exemplar electronic paystub that Divensi had sent him, which claimed falsely that money from his paycheck had been withheld and contributed to his 401k plan. VICTIM A further produced an email chain between him/her and SAMAL, in which SAMAL claimed that a payment plan would be necessary

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to compensate VICTIM A for his/her losses. SAMAL did not thereafter make any effort to establish such a payment plan or to respond to follow-up inquiries from VICTIM A.

18. On September 6, 2018, Special Agent Sarah Cloeter with the U.S. Department of State spoke with a representative at the 401k plan administrator used by Divensi (the "401k plan representative"). The 401k plan representative told SA Cloeter that Divensi stopped making payments into the 401k plan in or around 2016. The 401k plan representative also told SA Cloeter that the plan "received numerous phone calls and emails from employees of Divensi asking to get their money out," including from employees who had been led to believe (falsely) that money from their paychecks was being sent to the 401k plan. The 401k plan representative further stated that the trustees of the 401k plan account were SAMAL and WITNESS A. The 401k plan representative also stated that the plan trustees became unresponsive to requests for clarification from the 401k plan administrator.

19. On or around October 9, 2018, I interviewed an individual referred to herein as WITNESS D, who managed accounts payable and receivable and other financial matters for Divensi until his/her departure from the Divensi in the spring of 2018. WITNESS D told me that he was one of the employees responsible for processing employee paychecks and transferring amounts withheld from paychecks to the 401k plan administrator. WITNESS D admitted that Divensi did not transfer to the 401k plan administrator amounts that it had withheld from employee paychecks, despite asserting in the paychecks that the amounts had been withheld for the relevant employees' 401k plan contributions. WITNESS D told me that he/she did not make those contributions because SAMAL did not authorize him/her to do so, purportedly because of Divensi's need to cover cost overruns in other aspects of its business by using the misappropriated funds.

20. WITNESS D also told me that he/she communicated with SAMAL over email about the missing 401k contributions during the period of time that SAMAL was

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

outside the United States, in order to receive instructions from SAMAL about how to address complaints from former employees about their missing 401k contributions.[10]

21. There is probable cause to believe that the SUBJECT DEVICE will contain evidence of SAMAL's involvement in the diversion of employee 401k funds, including his email instructions to his employees like WITNESS D, his communications with employees who complained about missing funds, and his receipt of inquiries from the 401k plan administrator about employees whose funds had not properly been withheld by Divensi. As set out above, WITNESS D and others at SAMAL's companies have told investigators that they communicated with SAMAL over email during the time that he was overseas. WITNESS D has also told investigators that SAMAL conducted some financial transactions remotely from India.

22. On or about August 28, 2018, SAMAL flew from India to the United States, via Frankfurt. Upon arrival at Sea-Tac Airport, he was arrested on an arrest warrant issued by the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington.

23. Acting pursuant to their border-search authority, law-enforcement agents asked SAMAL for the password to the SUBJECT DEVICE, which he provided to them. Apart from confirming the functionality of the password and the SUBJECT DEVICE, the agents did not conduct a border examination of the SUBJECT DEVICE. Instead, in light of the pending criminal investigation, the government has elected to apply for the instant search warrant.

24. When conducting the requested search, however, the government respectfully submits that it has the authority to use the password provided by SAMAL

---

[10] WITNESS D told me that, in the event that individual employees would come forward to complain about their missing 401k funds, Divensi took the approach that the "squeaky wheel gets the grease." In effect, Divensi would attempt to address the complaints of employees when it received those complaints by belatedly making 401k contributions. Other than addressing these complaints, Divensi did not make any systematic effort to inform employees that their 401k contributions had not been made, and that the representations in their paychecks therefore had been false.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

pursuant to the agents' exercise of their border-search authority. The government seeks to use that password in lieu of electronically unlocking the SUBJECT DEVICE using external technology, which can create unnecessary costs and risks regarding the retrieval of data from the device.

25. The SUBJECT DEVICE is currently stored as evidence at the U.S. Department of Homeland Security, Homeland Security Investigations (HSI)'s offices in Seattle, Washington. In my training and experience, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE came into the possession of the government.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities on a digital device, namely the SUBJECT DEVICE. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

27. **Probable cause**. Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that there is probable cause to believe that the SUBJECT DEVICE contains evidence of the crimes under investigation, and indeed has been used as an instrumentality of those offenses. For the reasons explained above, there is probable cause to believe that the SUBJECT DEVICE contains evidence of SAMAL's location and activities during the time period that he was outside the United States, which may tend to evidence the crimes of Unlawful Flight from Prosecution and SAMAL's consciousness of guilt (i.e., his desire to flee from being charged with) the crimes of Visa Fraud and Conspiracy. In addition, there is probable cause to believe that SAMAL used the SUBJECT DEVICE to transfer assets

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

overseas after receiving payments from Synapse, and to communicate with WITNESS D and other employees about misappropriated employee 401k contributions.

28. There is, therefore, probable cause to believe that evidence of the crimes under investigation exist and will be found on the SUBJECT DEVICE, for at least the following reasons.

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. **Forensic evidence**. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes under investigation, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICE because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

SEARCH TECHNIQUES

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying the SUBJECT DEVICE, and will specifically authorize a later review of the media or information consistent with the warrant.

31. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of the SUBJECT DEVICE, and to conduct searches of the SUBJECT DEVICE and/or the forensic image of the SUBJECT DEVICE thereafter:

Processing the Search Sites and Securing the Data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICE.

b. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the SUBJECT DEVICE.

c. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

Searching the Forensic Images

d. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

32. The government understands that SAMAL has been represented by counsel since at least 2017 in connection with the criminal investigation. In light of the possibility that the SUBJECT DEVICE may contain privileged materials, the government will use a "taint" team, consisting of law-enforcement officers who have had no role in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the investigation and will have no continuing role in the investigation, to review the data from the SUBJECT DEVICES for non-privileged information and to filter out privileged information, including information that falls under Attachment B, as further described below.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B.

Dated this 26 day of October, 2018.

RICHARD LIN, Affiant
SPECIAL AGENT
U.S. DEPARTMENT OF STATE

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 26th day of October, 2018.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

A black Hewlett Packard Spectre laptop bearing serial number 5CD74295HB (hereinafter the SUBJECT DEVICE). The SUBJECT DEVICE is currently stored as evidence at the U.S. Department of Homeland Security, Homeland Security Investigations, office in Seattle, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Items to Be Seized

Evidence, fruits, and/or instrumentalities of the commission of the following crimes: Title 18, United States Code, Section 1956 (Laundering of Monetary Instruments), Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, Section 1073 (Flight to Avoid Prosecution), Title 18, United States Code, Section 1546 (Visa Fraud), and Title 18, United States Code, Section 371 (Conspiracy), those violations occurring between 2012 and the present, including:

a. Files, records, and other items relating to the Government's investigation into Pradyumna K. Samal, Divensi, Inc., or Azimetry, Inc., regarding applications for visas and other forms of legal status in the United States, including but not limited to correspondence and documents regarding potential witnesses and evidence, the financial proceeds of the conduct under investigation, and international travel to avoid prosecution in connection with the investigation.

b. Files, records, and other items relating to the sale of assets owned by Divensi, Inc., Azimetry, Inc., and/or Divensi Technology Inc. to Synapse, including documents and correspondence regarding the scope of the sale, covenants with regard to accounts payable and receivable, the transfer of client accounts and payments, and the treatment of client payments following transfer.

c. Files, records, and other items relating to the disposition of funds requested by employees to be withheld from paychecks for deposit in a company-sponsored 401k plan.

d. Files, records, and other items relating to location and international travel, including location data, wireless networks accessed, browsing history, and photographs.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In light of the possibility that the SUBJECT DEVICE may contain privileged materials, the government will use a "taint" team, consisting of law-enforcement officers who have had no role in the investigation and will have no continuing role in the investigation, to review the data from the SUBJECT DEVICES for non-privileged information and to filter out privileged information, including information that falls under Attachment B, as further described below.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EXHIBIT A

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

SUBJECT DEVICES, as further described in Attachments A-1 and A-2

Case No. MJ18-404

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-1 and A-2, which are attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 371,1546, 1341, 1073, 1512	Conspiracy to Defraud the United States, Visa Fraud, Mail Fraud, Unlawful Flight to Avoid Prosecution, Obstruction of Justice

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT MICHAEL RUFFIER, U.S. STATE DEPT

Printed name and title

Sworn to before me and signed in my presence.

Date: 30 August 2018

Judge's signature

City and state: SEATTLE, WASHINGTON

JAMES P. DONOHUE, U.S. MAGISTRATE JUDGE

Printed name and title

2016R00055

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, MICHAEL RUFFIER, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of digital devices, hereinafter the "SUBJECT DEVICES," which are currently in law enforcement possession, and the extraction from those devices of electronically stored information described in Attachment B.

2. I am a Special Agent of the Diplomatic Security Service ("DSS"), which is an agency of the United States Department of State ("State Department"), and I have been so employed for over 8 years. I am presently assigned to the Seattle Resident Office. I am empowered under 22 U.S.C. § 2709 to investigate visa frauds, as well as to apply for and serve federal arrest and search warrants. My previous assignments with DSS include the San Francisco Field Office, U.S. Embassy Baghdad, Iraq, U.S Consulate Ho Chi Minh City, Vietnam, and the Seattle Resident Office, along with numerous long-term temporary duty assignments to locales throughout the Middle East and South Central Asia. I also have a Bachelor's Degree in Business from the University of Oregon.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for search warrants, it does not set forth each

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1546 (visa fraud), Title 18, United States Code, Section 1341 (Mail Fraud), Title 18, United States Code, 1073 (Flight to Avoid Prosecution), and Title 18, United States Code, Section 1512 (Obstruction of Justice) will be found on the SUBJECT DEVICES.

IDENTIFICATION OF THE SUBJECT DEVICE TO BE EXAMINED

5. The SUBJECT DEVICES are:

a. An Apple iPhone 7-plus, bearing model number MN5M2LL/A and serial number F2LSFWS0HFYF (hereinafter SUBJECT DEVICE 1). On August 28, 2018, SUBJECT DEVICE 1 was seized from the person of PRADYUMNA K. SAMAL incident to his arrest. SUBJECT DEVICE 1 is currently stored as evidence at the U.S. Department of Homeland Security, Homeland Security Investigations, office in Seattle, Washington.[1]

b. An Apple iPhone X, bearing model number MQA82LL/A and serial number F2PVWG1BJCL6 (hereinafter SUBJECT DEVICE 2). On August 28, 2018, SUBJECT DEVICE 2 was seized from the person of PRADYUMNA K. SAMAL incident to his arrest. SUBJECT DEVICE 2 is currently stored as evidence at the U.S. Department of Homeland Security, Homeland Security Investigations, office in Seattle, Washington.

6. SUBJECT DEVICES 1 and 2 are collectively referred to herein as the "SUBJECT DEVICES." The warrants would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

STATEMENT OF PROBABLE CAUSE

7. Since in or about 2015, the United States Department of State has investigated PRADYUMNA K. SAMAL ("SAMAL") for submitting false and fraudulent

[1] SUBJECT DEVICE 1 previously was searched by agents on or about October 5, 2017, pursuant to a search warrant issued by the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington. The returns from that warrant reflect that SUBJECT DEVICE 1 is assigned a telephone number by the service provider T-Mobile in the United States.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

applications for nonimmigrant workers to the United States Citizenship and Immigration Services ("USCIS"). The Complaint in the matter of *United States v. Samal*, MJ18-190, is attached hereto as Exhibit A and incorporated as if fully set forth herein. As set out in the Complaint, SAMAL has served as the Chief Executive Officer of two companies that together petitioned for over one-hundred-and-thirty (130) foreign nationals to work temporarily in the United States pursuant to the H-1B program.[2] SAMAL's companies' petitions included forged and false materials, which SAMAL and others acting at his direction included in order to induce USCIS to approve the applications.

8. On or about October 5, 2017, law-enforcement agents searched the business offices of SAMAL's companies pursuant to search warrants issued by the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington, under cause number MJ17-413. At those offices, agents found extensive evidence of the visa-fraud scheme and SAMAL's involvement in the scheme, including emails in which SAMAL circulated, to his colleagues, copies of documents onto which he had affixed forged signatures, and which later were included in applications that his companies filed with USCIS. Law-enforcement agents also found evidence of SAMAL's consciousness of guilt and obstruction of justice, including, most significantly, the removal of fraudulent documents from copies of visa petitions that SAMAL's companies kept in hard-copy form at the offices.[3] In particular, law-enforcement agents discovered that all but one of the hard-copy petition files were missing forged end-client letters and statements of work, which SAMAL's companies had sent USCIS.

---

[2] Under Section 101(a)(15)(H) of the Immigration and Nationality Act ("INA"), U.S.-based employers can petition for foreign nationals to enter the United States and work under specialty occupations.

[3] USCIS requires companies that submit visa petitions to keep hard copies of the petition files at their offices for specified periods of time, in order to facilitate periodic in-person "audits" by USCIS. Notwithstanding the requirement on companies to maintain hard copies of petitions, USCIS itself keeps copies of petition materials for some period of time after filing. By comparing the copies of the petitions sent to USCIS with the copies that SAMAL's companies maintained at their offices, law-enforcement agents discovered that almost all of the hard-copy files were missing incriminating documents that had been sent to USCIS.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

9. On February 15, 2018, SAMAL flew from Seattle, Washington to New Delhi, India. Records produced by the airline that he used show that he purchased the ticket less than two hours before the flight was scheduled to depart Seattle. In my training and experience, and in light of the time ordinarily required for a traveler to check-in for a flight and clear security before boarding, SAMAL appears to have purchased the ticket at the Seattle-Tacoma airport. SAMAL also purchased a return ticket, under which he would have returned to Seattle from New Delhi on March 5, 2018. In my training and experience, subjects of federal investigations sometimes purchase return tickets that they do not intend to use, in order to avoid law-enforcement scrutiny associated with a one-way international journey.

10. Indeed, SAMAL did not return to the United States from India on March 5, 2018, as scheduled. Nor did SAMAL leave India between February 2018 and his flight on or about August 28, 2018. Since SAMAL left the United States for India, law-enforcement agents have discovered several facts, which establish probable cause to believe that he left the United States for India because of his consciousness of guilt regarding the crimes under investigation, and in order to avoid prosecution for those crimes. As explained below, there is probable cause to believe that the SUBJECT DEVICES contain evidence regarding each of the facts below, including the extent to which these facts serve as evidence of the crimes under investigation and SAMAL's intent to flee prosecution for those crimes.

11. ***First***, SAMAL left the United States abruptly, just days after a High Ranking Executive proffered evidence against him to agents and days before an Outside Consultant was scheduled to provide evidence against him. More specifically:

a. The High Ranking Executive: On January 30, 2018, law-enforcement agents conducted a proffer interview of a former High Ranking Executive at SAMAL's companies. The High Ranking Executive was represented by counsel at that interview. Evidence from the search warrant referred to above, as well as other evidence

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

gathered over the course of the investigation,[4] revealed the High Ranking Executive's role in preparing visa-application materials that SAMAL's companies sent to USCIS. In particular, numerous emails showed that the High Ranking Executive put together application materials that included false documents and recruited foreign nationals to the companies.

The High Ranking Executive told agents that, in his role at the companies, he worked directly with foreign nationals who were the subject of the fraudulent H-1B petitions. He told agents that he was aware that the petition packets relating to those foreign nationals included false information in them, insofar as the packets claimed that the foreign nationals had been assigned to projects for CLIENT A or CLIENT B. He told agents that he did not prepare the fraudulent application materials himself, but that SAMAL and an Outside Consultant hired by the companies, did the bulk of the work with regard to the preparation of fraudulent petition packets.

The High Ranking Executive also told agents about statements that SAMAL made to him during their professional relationship. For instance, the High Ranking Executive recounted that he talked to SAMAL about foreign nationals who arrived in the United States of fraudulently-obtained visas, and then confronted SAMAL about the lack of work for them. The High Ranking Executive told agents that SAMAL represented to the High Ranking Executive that CLIENT A's Executive had authorized SAMAL to represent (falsely) in USCIS filings that CLIENT A's Executive had agreed to use named foreign nationals on projects for CLIENT A.[5] The High Ranking Executive also told agents that SAMAL said "this is how this industry works," with regard to the submission of false and forged information to USCIS.[6]

---

[4] During the investigation, law-enforcement agents interviewed several foreign nationals who were the subject of petitions filed by SAMAL's companies (i.e., the foreign nationals who SAMAL's companies sought to employ as nonimmigrant workers under the H-1B program, and who SAMAL's companies falsely claimed had been placed at projects for CLIENT A and CLIENT B, as described in the Complaint). Law-enforcement agents also searched the email accounts of some of SAMAL's companies' employees and executives pursuant to warrants issued by the Honorable Brian A. Tsuchida, Chief United States Magistrate Judge for the Western District of Washington, under cause number MJ16-313.

[5] As explained in the Complaint, CLIENT A denied that it ever authorized SAMAL or anyone else at SAMAL's companies to misappropriate the identity of CLIENT A's Executive (or CLIENT A generally) in furtherance of SAMAL's visa fraud.

[6] As explained in the Complaint, the documentary evidence corroborates the High Ranking Executive's account of SAMAL's knowledge and participation in the creation of false documents in visa petitions. However, the High Ranking Executive had made certain false statements to the Government in connection with its investigation. For instance, before entering into a proffer agreement, the High Ranking Executive initially claimed to agents that he only saw fraudulent end-client letters in hardcopy form only, when the companies' Outside Consultant was preparing for them to be sent to USCIS. In truth and in fact, email records showed that the High Ranking Executive received electronic copies of those end-client letters. The High Ranking Executive also initially claimed that he believed the end-client letters were authentic – a fact that he later admitted was false. Email records also show that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Upon arriving in India on or about February 17, 2018, SAMAL sent the High Ranking Executive a WhatsApp communication stating "here in India! Let me know if I can call you?" Counsel for the High Ranking Executive provided a screenshot of that WhatsApp communication to the government. In my training and experience, and based on records produced by WhatsApp regarding SAMAL's account, SAMAL uses a WhatsApp account that is registered to a telephone number registered by an Indian cellular service provider.[7] Even though the telephone number is registered by an Indian service provider, the WhatsApp account still is accessible from any of SAMAL's digital devices, including the SUBJECT DEVICES, through the use of the WhatsApp application. There is therefore probable cause to believe that the SUBJECT DEVICES contain evidence of SAMAL's communications over WhatsApp (and otherwise, including through phone logs reflecting any follow-up calls) with the High Ranking Executive.

b. The Outside Consultant:[8] On January 29, 2018, agents served a subpoena on the companies' Outside Consultant, requiring that Outside Consultant to testify in connection with the investigation. The subpoena directed the Outside Consultant to appear on February 21, 2018, though the Outside Consultant failed to appear on that date. The Outside Consultant finally met with the government pursuant to the proffer agreement on March 27, 2018; her attorney was present during the interview.

The Outside Consultant told agents that she had spoken to SAMAL several times in the months before her proffer interview. She recounted that she spoke with SAMAL after being served with a subpoena and that SAMAL warned her to "be careful" about the information she provided the government. She also said that, about three to four weeks before her proffer interview (i.e., about three to four weeks before March 27, 2018), she called SAMAL to discuss outstanding amounts he owed her for services previously rendered by her. During that conversation, SAMAL asked her for an update about the status of the criminal investigation, and requested that she keep him apprised of

---

the High Ranking Executive engaged in acts of dishonesty when carrying out the visa-fraud scheme, including by directing foreign nationals to lie to U.S. consular officers at consulate interviews.

[7] As explained above, SUBJECT DEVICE 1 previously was searched by law-enforcement agents, who determined that the phone is assigned to a U.S.-based service provider. There is therefore probable cause to believe that SUBJECT DEVICE 2, which SAMAL carried with him into the United States from India, is the device to which the Indian telephone number is assigned (and is one of the devices SAMAL used to register the WhatsApp account he later used to communicate with the High Ranking Executive and others).

[8] The Outside Consultant is a former attorney, barred in the State of Washington, who was disbarred from practice in this State and before the Department of Homeland Security, as a result of acts involving dishonesty. The Outside Consultant has also admitted to engaging in dishonest conduct, insofar as she conspired with SAMAL and other clients in similar business enterprises as SAMAL to send false materials to USCIS in connection with visa applications. The Outside Consultant admitted in a second interview that she discussed the contents of her first proffer interview with potential subjects of the government's investigation, which was contrary to the covenants in her proffer agreement with the government.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

any developments. Based on the facts set out above, there is probable cause to believe that the conversation between SAMAL and the Outside Consultant took place after SAMAL fled to India, on the same cellular telephone number that the Outside Consultant otherwise used to communicate with SAMAL. Voicemails previously found on SUBJECT DEVICE 1 establish that the Outside Consultant repeatedly called SAMAL on SUBJECT DEVICE 1, to inquire about amounts that SAMAL owed her for services previously rendered.

The Outside Consultant also admitted engaging in apparently criminal conduct with SAMAL, including efforts to obstruct the government's investigation. Specifically, she told agents that SAMAL initially misrepresented to her that the information in petitions about purported projects at CLIENT A and CLIENT B was accurate, but that she later discovered that it was not. Even after discovering that the information was inaccurate, however, the Outside Consultant continued to prepare petitions containing that false information. She claimed that she continued to engage in the criminal conduct she did not want to jeopardize her ongoing business relationship with the companies.

The Outside Consultant also admitted that she helped destroy the documents referred to in paragraph 9. Specifically, she told agents that she and approximately two other employees of SAMAL's companies met for one week in a conference room at the companies' offices in or around the summer of 2015, approximately three or four months after SAMAL became aware of the government's investigation, and reviewed all of the hardcopy visa-petition files stored at the companies' offices. The Outside Consultant told agents that she and the other employees removed fraudulent documents from the hardcopies of visa petitions that SAMAL's companies kept, and that she understood that the fraudulent documents would later be destroyed. She claimed that the employees purported to operate under the pretext of reorganizing the files. She also recalled that SAMAL periodically checked in with the employees and the Outside Consultant about the status of their efforts to remove the incriminating materials from the files.

12. ***Second***, following SAMAL's departure from the United States, agents learned he was selling off portions of his companies' United States operations. For instance, in or about April 4, 2018, a company named Synapse Technologies LLC filed an "amended petition" with USCIS for a foreign national who previously was the subject of a petition filed by SAMAL's company, Azimetry.

13. The petition filed by Synapse Technologies LLC claimed that pursuant to a bill of sale attached to the petition, "***Synapse has acquired all rights and liabilities of***

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Azimetry, Inc. and is its successor in interest." (emphasis added). The bill of sale was dated February 9, 2018 – ***six days before SAMAL departed the United States*** – and had been signed by SAMAL. It purported to assign Azimetry's interest in its customer contracts and other rights related to its H-1B staffing business to Synapse Technologies LLC.

14. Similarly, on or about May 23, 2018, a USCIS officer informed me over email that Synapse Technologies LLC had filed an amended petition for a foreign national who previously was the subject of a petition filed by Divensi. The USCIS officer informed investigative agents that the petition claimed that Synapse Technologies LLC was acting as an "FKA" or a "formerly known as" of Divensi, indicating that SAMAL sold Divensi's rights and interest in its H-1B business to Synapse Technologies LLC on or around the time that he fled from the United States.

15. There is probable cause to believe that the SUBJECT DEVICES contain evidence of SAMAL's efforts to dispossess his companies of their H-1B-related operations in the United States, and that such efforts may evidence the crimes under investigation, as well as SAMAL's efforts to flee from prosecution. The petitions filed by Synapse Technologies LLC referred to above were filed *after* SAMAL left the United States for India, meaning that any efforts between SAMAL and Synapse Technologies to coordinate the transfer of aspects of the business would have occurred remotely, over email and other messaging applications. Communications involving SAMAL with regard to the H-1B operations that his companies transferred to Synapse Technologies LLC may speak to SAMAL's beliefs regarding the authenticity of the underlying petitions previously filed by his companies, his efforts to distance himself from those petitions (by selling off business concerns involving those petitions), and his efforts to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

distance himself from the U.S. operations generally (by selling off the U.S.-based aspects of his business, which arose from placing H-1B workers at end clients).[9]

16. ***Third***, following his departure from the United States, SAMAL communicated regularly over the encrypted messaging application WhatsApp. Connection records produced to the government by WhatsApp show that SAMAL regularly exchanged messages with an individual referred to herein as "A.M.," who previously wired funds to accounts owned by SAMAL.[10]

17. There is probable cause to believe that the content of the communications between SAMAL and A.M. will evidence SAMAL's consciousness of guilt about the offenses under investigation, and his intent to evade prosecution for those offenses, in light of the fact that A.M. had worked with SAMAL and had a pre-existing relationship with SAMAL's family, which involved the transfer of hundreds of thousands of dollars by A.M. to SAMAL's family. Other WhatsApp messages found on the SUBJECT DEVICES also may reflect evidence of SAMAL's whereabouts after leaving the United States, including through location data regarding those communications, the content of those communications, and the identity of those with whom he communicated.

18. ***Fourth***, there is probable cause to believe that SAMAL made a false statement to U.S. government official during the time that he was away from the United States, and that the SUBJECT DEVICES contain evidence of his state of mind when making that statement. Specifically, in addition to the criminal investigation referred to in the Complaint, SAMAL's companies have been investigated by the United States Department of Labor ("DOL").

---

[9] There is also probable cause to believe that SAMAL used the SUJECT DEVICES to conduct business operations in India, which serves as evidence of his intent to flee from prosecution insofar as he intended to transfer his commercial interests away from the United States and to India. For instance, SAMAL and his wife are both directors of Divensi Solutions Private Ltd., an Indian company with offices that corporate documents establish are in Bhubaneswar, India.

[10] More specifically, account records for one of SAMAL's personal bank accounts reflect over $300,000 in transfers from accounts associated with A.M. between January 2017 and November 2017. To the extent memo lines were reflected for the transfers, those memo lines referred to the transferred funds as "family support," or "family maintenance."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. In connection with that investigation, a DOL investigator reported that she spoke with SAMAL over the telephone on May 21, 2018, and claimed that SAMAL would return to the United States on or about May 30. As explained above, he did not in fact return on that date. Information on the SUBJECT DEVICES can serve as evidence of SAMAL's actual intent, at the time of the phone call with the DOL investigator and thereafter, to return (as he claimed) on or about May 30, 2018. Evidence of such intent may include communications with others about his travel plans, actual efforts to secure such travel, and evidence of his intent with regard to the pending investigation.

20. In addition to the probable cause that the SUBJECT DEVICES contain evidence (e.g., communications) regarding the specific facts referred to above, there is also probable cause to believe that the SUBJECT DEVICES contain evidence of SAMAL's location since his departure from the United States, and that such evidence can demonstrate his consciousness of guilt of the underlying offenses and/or his intent to flee from prosecution.

21. Location data found on the SUBJECT DEVICES can shed light on whether SAMAL traveled to cities in India in which he attempted to build his business operations or establish residency, or whether he traveled to any countries outside India where he attempted to make similar efforts. In addition to the phones' location data, multimedia, such as photographs and videos, on the phones can evidence who SAMAL associated with in India, including whether he attempted to associate with potential witnesses to the federal criminal case, such as the High Ranking Executive. Finally, as set out below, there is probable cause to believe SAMAL used the SUBJECT DEVICES as instrumentalities of his crimes, to the extent he used the device assigned an American telephone number to communicate with the Outside Consultant and used the device assigned an Indian telephone number to communicate over WhatsApp.

22. On or about August 28, 2018, SAMAL flew from India to the United States, via Frankfurt. Upon arrival at Sea-Tac Airport, he was arrested on an arrest

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

warrant issued by the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington.

23. Acting pursuant to their border-search authority, law-enforcement agents asked SAMAL for the passwords to the SUBJECT DEVICES, which he provided to them. Apart from confirming the functionality of the passwords and the phones, the agents did not conduct a border examination of the SUBJECT DEVICES. Instead, in light of the pending criminal investigation, the government has elected to apply for the instant search warrants. When conducting the requested searches, however, the government respectfully submits that it has the authority to use the passwords provided by SAMAL pursuant to the agents' exercise of their border-search authority. The government seeks to use those passwords in lieu of electronically unlocking the SUBJECT DEVICES using external technology, which can create unnecessary costs and risks regarding the retrieval of data from the devices.

24. The SUBJECT DEVICES are currently stored as evidence at HSI's offices in Seattle, Washington. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of the government.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, discussions with computer forensic technicians, and open source research, I know that the SUBJECT DEVICES have

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

capabilities that allow it to serve as the following: wireless mobile communication device, digital camera, digital video camera, GPS navigation device, storage of digital information to include photos, videos, documents, contact lists, emails, Internet browser history, software, and other digital data. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, as well as evidence that the device was used as an instrumentality of a crime.

CELLPHONES AND WIRELESS COMMUNICATIONS DEVICES

27. Cellphones or "Wireless Communication Devices" includes cellular telephones and other devices such as tablets (e.g. iPads and other similar devices) used for voice and data communication through cellular or Wi-Fi signals. These devices send signals through networks of transmitter/receivers, enabling communication with other wireless devices or traditional "land line" telephones. Many such devices can connect to the Internet and interconnect with other devices such as car entertainment systems or headsets via Wi-Fi, Bluetooth or near field communication (NFC). In addition to enabling voice communications, wireless communication devices offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books" or "contact lists;" sending, receiving, and storing short message service (SMS) and multi-media messaging service (MMS) text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; and storing dates, appointments, and other information on personal calendars.

28. Based upon my training and experience, all of these types of information may be evidence of crimes under investigation. Stored e-mails and text messages not only may contain communications relating to crimes, but also help identify the participants in those crimes. Address books and contact lists may help identify co-conspirators. Similarly, photographs on a cellular telephone may help identify the device user and co-conspirators, either through his or her own photographs, or through

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

photographs of friends, family, and associates. Digital photographs also often have embedded location data GPS information that identifies where the photo was taken. This location information is helpful because, for example, it can show where coconspirators meet, where they travel, and where assets might be located. Calendar data may reveal the timing and extent of criminal activity.

29. A cellphone used for cellular voice communication will also typically contain a "call log" or "stored list of recent, received, sent or missed calls" which records the telephone number, date, and time of calls made to and from the phone. The stored list of recent received, missed, and sent calls is important evidence. It identifies telephones recently in contact with the telephone user and may help identify co-conspirators, establish a timeline of events and/or identify who was using the phone at any particular time.

30. In addition, wireless communication devices will typically have an assigned number and identifying serial number such as an ESN, MIN, IMSI or IMEI number that identifies the particular device on any network. This identifying information may also include the device's assigned name (as assigned by the user) and network addresses such as assigned IP addresses and MAC address. I know based on my training and experience that such information may be important evidence of who used a device, when it was used, and for what purposes it may have been used. This information can be used to obtain toll records and other subscriber records, to identify contacts by this telephone with other telephones, or to identify other telephones used by the same subscriber or purchased as part of a package.

31. Many wireless communication devices including cellular telephones such as iPhones, iPads, Android phones, and other "smart phones" as well as tablet devices such as Apple iPads may also be used to browse and search the Internet. These devices may browse and search the internet using traditional web browsers such as Apple's Safari browser or Google's Chrome browser as well as through third-party applications such as Facebook, Twitter and others that also provide the ability to browse and search the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

internet. Based on my training and experience, I know that internet browsing history may include valuable evidence regarding the identity of the user of the device. This evidence may include online user names, account numbers, e-mail accounts and bank accounts as well as other online services. Internet browsing history may also reveal important evidence about a person's location and search history. Search history is often valuable evidence that may help reveal a suspect's intent and plans to commit a crime or efforts to hide evidence of a crime and may also help reveal the identity of the person using the device.

32. Cellphones and other wireless communication devices are also capable of operating a wide variety of communication applications or "Apps" that allow a user to communicate with other devices via a variety of communication channels. These additional communication channels include traditional cellular networks, voice over internet protocol, video conferencing (such as FaceTime and Skype), and a wide variety of messaging applications (such as SnapChat, What'sApp, Signal, Telegram, Viber and iMessage). I know based on my training and experience that there are hundreds of different messaging and conferencing applications available for popular cellular telephones and that the capabilities of these applications vary widely for each application. Some applications include end-to-end encryption that may prevent law enforcement from deciphering the communications without access to the device and the ability to "unlock" the device through discovery of the user's password or other authentication key.

33. Other communication applications transmit communications unencrypted over centralized servers maintained by the service provider and these communications may be obtained from the service provider using appropriate legal process. Other applications facilitate multiple forms of communication including text, voice, and video conferencing. Information from these communication apps may constitute evidence of the crimes under investigation to the extent they may reveal communications related to the crime or evidence of who the user of the device was communicating with and when

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

those communications occurred. Information from these communication apps may also reveal alias names used by the device owner that may lead to other evidence.

34. I know based on my training and experience that obtaining a list of all the applications present on a cellphone may provide valuable leads in an investigation. By determining what applications are present on a device, an investigator may conduct follow-up investigation including obtaining subscriber records and logs to determine whether the device owner or operator has used each particular messaging application. This information may be used to support additional search warrants or other legal process to capture those communications and discover valuable evidence.

35. Cellphones and other wireless communication devices may also contain geolocation information indicating where the device was at particular times. Many of these devices track and store GPS and cell-site location data to provide enhanced location based services, serve location-targeted advertising, search results, and other content. Numerous applications available for wireless communication devices collect and store location data. For example, when location services are enabled on a handheld mobile device, many photo applications will embed location data with each photograph taken and stored on the device. Mapping applications such as Google Maps may store location data including lists of locations the user has entered into the application. Location information may constitute evidence of the crimes under investigation because that information may reveal whether a suspect was at or near the scene of a crime at any given moment and may also reveal evidence related to the identity of the user of the device. Searching a cellular phone or wireless communication device is frequently different than conducting a search of a traditional computer. Agents and forensic examiners will attempt to extract the contents of the cellular phone or wireless communication device using a variety of techniques designed to accurately capture the data in a forensically sound manner in order to make the data available to search for the items authorized by the search warrant. This may involve extracting a bit-for-bit copy of the contents of the device or, if such an extraction is not feasible for any particular device, the search may

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

involve other methods of extracting data from the device such as copying the device's active user files (known as a logical acquisition) or copying the device's entire file system (known as a file system acquisition). If none of these methods are supported by the combination of tools available to the examiner and the device to be searched, the agents and examiners may conduct a manual search of the device by scrolling through the contents of the device and photographing the results.

36. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

37. As set forth above, there is probable cause to believe that the SUBJECT DEVICE has been used as an instrumentality of, and therefore contains evidence of, the crimes under investigation. More specifically, and as described in further detail above:

a. The Outside Consultant communicated via telephone and text message with SAMAL about topics that included the status of the criminal investigation, including after she proffered evidence to the government.

b. SAMAL used the WhatsApp messaging application to send at least one known message to the High Ranking Executive after SAMAL arrived in India. In that message, SAMAL asked the High Ranking Executive if he could engage in a telephone call – a call which there is probable cause to believe took place using one of the SUBJECT DEVICES.

c. SAMAL also used the WhatsApp application to communicate extensively with A.M., an individual who lives in the United States and who has a preexisting financial relationship with SAMAL.

d. SAMAL used the SUBJECT DEVICES to conduct business, including business relating to the sale of the aspects of his U.S. business operations that were under investigation to Synapse Technologies LLC, and business relating to the development of his Indian operations.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SEARCH TECHNIQUES

38. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICES, and will specifically authorize a review of the media or information consistent with the warrant.

39. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES pursuant to this warrant as follows:

a. Securing the Data

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICE.

ii. Law enforcement will only create an image of data physically present on or within the SUBJECT DEVICE. Creating an image of the SUBJECT DEVICE will not result in access to any data physically located elsewhere. However, if the SUBJECT DEVICE has previously connected to devices at other locations, it may contain data from those other locations.

b. Searching the Forensic Images

i. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

40. The government understands that SAMAL has been represented by counsel since at least 2017 in connection with the criminal investigation. In light of the possibility that the SUBJECT DEVICES may contain privileged materials, the government will use a "taint" team, consisting of law-enforcement officers who have had

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

no role in the investigation and will have no continuing role in the investigation, to review the data from the SUBJECT DEVICES for non-privileged information that falls under Attachment B, as further described below.

CONCLUSION

41. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

Dated this 30 day of August, 2018.

MICHAEL RUFFIER, Affiant
SPECIAL AGENT
U.S. DEPARTMENT OF STATE

Subscribed and sworn to before me this 30th day of August, 2018.

JAMES P. DONOHUE
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

The property to be searched is an Apple iPhone 7-plus, bearing model number MN5M2LL/A and serial number F2LSFWS0HFYF (hereinafter SUBJECT DEVICE 1). On August 28, 2018, SUBJECT DEVICE 1 was seized from the person of PRADYUMNA K. SAMAL incident to his arrest. SUBJECT DEVICE 1 is currently stored as evidence at the U.S. Department of Homeland Security, Homeland Security Investigations, office in Seattle, Washington.

This warrant authorizes the forensic examination of the SUBJECT DEVICE 1 for the purpose of identifying the electronically stored information described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

The property to be searched is an Apple iPhone X, bearing model number MQA82LL/A and serial number F2PVWG1BJCL6 (hereinafter SUBJECT DEVICE 2). On August 28, 2018, SUBJECT DEVICE 2 was seized from the person of PRADYUMNA K. SAMAL incident to his arrest. SUBJECT DEVICE 2 is currently stored as evidence at the U.S. Department of Homeland Security, Homeland Security Investigations, office in Seattle, Washington.

This warrant authorizes the forensic examination of the SUBJECT DEVICE 1 for the purpose of identifying the electronically stored information described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Section 1546 (visa fraud), Title 18, United States Code, Section 1341 (Mail Fraud), Title 18, United States Code, 1073 (Flight to Avoid Prosecution), and Title 18, United States Code, Section 1512 (Obstruction of Justice), including:

a. Correspondence relating to H-1B visa petitions, the transfer of business operations relating to H-1B visa petitions, the pending criminal investigation into false H-1B visa petitions, and travel to and from the United States, including text messages, WhatsApp messages, and electronic-mail communications regarding the content of visa petitions, pending criminal investigations and statements made in the context of those investigations, and travel plans;

b. Digital media, including photographs and videos, including digital media that depicts the locations of the device's user, potential witnesses to a criminal investigation, overseas business offices, overseas residences, and the device user's overseas associates;

c. Internet browser history, including logs of access to websites used in connection with the operation of businesses outside the United States;

d. Location data, including data reflecting travel outside the United States;

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The United States will use a filter team to ensure that only documents or evidence described in Attachment B will be turned over to investigative agents. The filter team shall not disclose the existence of or seize evidence or documents not covered by the warrant, excepting only exigent circumstances as defined by the Fourth Amendment.

When executing the warrant, the United States may use the passwords provided by the user of the SUBJECT DEVICE at the time that those devices were seized by law-enforcement agents incident to the user's arrest.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Magistrate Judge Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PRADYUMNA KUMAR SAMAL

Defendant.

CASE NO. MJ18-190

COMPLAINT for VIOLATION

Title 18, United States Code, Section 1546

BEFORE, Mary Alice Theiler, United States Magistrate Judge, U. S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE

Visa Fraud

On or about April 1, 2014, at Bellevue, within the Western District of Washington and elsewhere, the Defendant Pradyumna Kumar Samal ("SAMAL") did knowingly subscribe as true, under penalty of perjury, a false statement with respect to a material fact in a document required by the immigration laws and regulations of the United States, to wit, an I-129 Petition for Nonimmigrant Worker. To wit, SAMAL falsely claimed that the foreign-national beneficiary named in the petition, L.N., had been assigned to work at

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Azimetry, Inc.'s offices on a project for an end-client to which L.N. had not been assigned.

All in violation of Title 18, United States Code, Section 1546.

And the complainant states that this Complaint is based on the following information:

I, Richard Lin, being first duly sworn on oath, depose and say:

I. INTRODUCTION AND AFFIANT BACKGROUND

1. I am a Special Agent of the Diplomatic Security Service (DSS), which is an agency of the United States State Department, and I have been so employed for over 16 years. I am presently assigned to the Document and Benefit Fraud Task Force at DHS. This task force investigates sophisticated immigration frauds in the San Francisco Bay Area, and as such, I have received and continue to receive specialized training and instruction from State Department officers who issue entry visas to foreigners overseas and DHS officers who issue employment documents to foreigners already inside of the United States. I am empowered under 22 U.S.C. § 2709 to investigate visa frauds, as well as to apply for and serve federal arrest and search warrants. My previous assignments include postings in New York, DSS Headquarters - Washington, D.C., Karachi, Pakistan, Beirut, Lebanon, and Los Angeles, as well as numerous long-term temporary duty assignments throughout the Middle East and South Central Asia. Prior to DSS, I served in the U.S. Marine Corps Reserve and also have a Master's Degree in Public Administration from the University of Georgia.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrant and does not set forth all of my knowledge about this matter.

II. BACKGROUND AND SUMMARY OF PROBABLE CAUSE

3. Since 2015, the United States Department of State and the United States Department of Homeland Security have investigated two Washington State companies

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

named Divensi, Inc. ("Divensi") and Azimetry, Inc. ("Azimetry") (collectively the "SUBJECT COMPANIES") for committing suspected acts of visa fraud. As set out in additional detail below, at all times relevant to the investigation, the SUBJECT COMPANIES have provided information-technology services to corporate clients, including a variety of so-called "Fortune 500" companies (and recruiting firms retained by those companies), in the information-technology field. More specifically, at all times relevant to this investigation, the SUBJECT COMPANIES have hired employees with experience in the information-technology field, such as programmers, marketed those employees to corporate clients, and then placed those employees at corporate clients pursuant to contracts entered into between the SUBJECT COMPANIES and their clients (and/or their clients' agents).

4. The suspected fraud arises out of more than one hundred petitions for nonimmigrant workers that the SUBJECT COMPANIES filed with the United States Citizenship and Immigration Service ("USCIS"). In those filings, the SUBJECT COMPANIES petitioned for certain foreign nationals to receive so-called H-1B visas under Section 101(a)(15)(H) of the Immigration and Nationality Act, pursuant to which the foreign nationals would be permitted to live temporarily in the United States and work in positions that required specialized skills. The petitions under investigation claimed that the foreign nationals would be working at the SUBJECT COMPANIES' offices in Bellevue on projects for two of the SUBJECT COMPANIES' purported clients. The petitions included letters that purported to have been issued by those clients, purported to have been signed by those clients' representatives, and claimed that the foreign national named in the petition indeed had been assigned to a project for the client. In truth and in fact, the petitions' claims were false and the purported supporting documents were fabricated.

5. According to records maintained by the Secretary of State for Washington State, Samal incorporated Divensi in 2010 and Azimetry in 2011. At all times relevant to the investigation, the SUBJECT COMPANIES' corporate documents listed SAMAL

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as the Chief Executive Officer ("CEO"), the highest-ranking position in the corporate hierarchy.

6. As set out below, there is extensive probable cause to believe that, in his role as CEO of the SUBJECT COMPANIES, SAMAL conceived, directed, participated in, and then attempted to cover up the fraud. The evidence consists of emails produced by the SUBJECT COMPANIES' email service provider,[1] records found at the SUBJECT COMPANIES' erstwhile offices,[2] and interviews with the SUBJECT COMPANIES' former and current employees and contractors, including SAMAL himself. In short, SAMAL received and reviewed petitions before filing, affixed unauthorized signatures on letters that appeared to have been issued by others, directed employees to market foreign nationals to clients other than those named in the fraudulent petitions, and then lied to investigators and attempted to destroy evidence of the fraud.

III. BACKGROUND REGARDING H-1B WORK VISAS

7. The H-1B visa program is a program administered by USCIS. Under the program, employers in the United States may apply to USCIS to issue visas to foreign nationals under which those foreign nationals may enter the United States and work in a "specialty occupation" for the petitioning employer while in this country. In recent years, U.S. employers typically have sought H-1B visas for foreign nationals who have experience and post-graduate degrees in computer programming, biological sciences, and engineering. Because H-1B visas originally were designed to enable U.S. employers to use foreign nationals for certain narrow categories (i.e., "specialty occupation") of jobs in the absence of a large enough labor pool in the United States, H-1B visas are subject to strict issuance requirements, including quotas, certifications by the petitioning employers regarding wages, and lengthy processing times.

---

[1] The SUBJECT COMPANIES' email-service provider produced emails pursuant to a warrant issued by the Honorable Brian A. Tsuchida, United States District Court for the Western District of Washington, under cause number MJ16-313.

[2] In October 2017, law-enforcement agents searched the SUBJECT COMPANIES' offices in Bellevue, Washington, pursuant to two warrants issued by the Honorable Mary Alice Theiler, United States District Court for the Western District of Washington, under cause number MJ17-413.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. *Background Regarding Application Procedures for H-1B Visas*

8. In order to apply for an H-1B visa, a petitioning employer ordinarily must follow all of the following steps:

9. ***First***, the U.S. employer, acting as a petitioner, must submit a Labor Condition Application ("LCA") for Nonimmigrant Workers to the United States Department of Labor ("DOL") through an online portal. In the LCA, the employer must make certain attestations, including that employing a foreign national under an H-1B visa will not adversely affect the working conditions of similarly-situated U.S. workers (e.g., by depressing wages or interfering with a labor strike). The employer must also post a hardcopy or electronic notice of the LCA for ten days at the employer's office and at the offices of the end client (if any) where the foreign worker will work. In the event that DOL approves the LCA and determines that the American company qualifies to hire foreign workers, the petitioning employer is required to maintain the LCA onsite for inspection by immigration and law-enforcement officials. Based on my training and experience, petitioning companies typically will email copies of the LCA and supporting documentation to their employees, government officials upon request, and other companies with which they are engaged in business. Moreover, a copy of the LCA must be given to the H-1B worker no later than when he/she reports to work.

10. ***Second***, if and after the DOL approves a petitioning employer's LCA, the employer must submit to DHS a Petition for a Nonimmigrant Worker (referred to as an "I-129" form) for every foreign worker that it wishes to employ pursuant to an H-1B visa. The I-129 is a thirty-six (36) page application that USCIS makes available on its website at www.uscis.gov in a "fillable" portable document format ("PDF"). The form can be completed electronically and then saved to a digital device, after which it can either be printed and mailed to DHS or filed electronically.[3] The I-129 requires the petitioning

[3] In the event that an I-129 is filed electronically, DHS issues an "electronic receipt" – a digital acknowledgment of the filing of an I-129 – to the petitioning employer.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

employer to disclose, *inter alia*, the foreign national employee's name and biographical information, the wage that the employer proposes to pay the foreign national, the business address at which the foreign national will work, and information about the employer itself.

11. The I-129 includes numerous sections that require the petitioning employer to certify the truthfulness of the information contained therein and that warn the petitioner about the consequences of including false information in the application.[4] During the application process, USCIS informs the petitioner that it reserves the right to verify any information submitted, including through written and telephonic correspondence and "unannounced physical site inspections of residences and places of employment and interviews." Once the I-129 is submitted, USCIS adjudicates it based on the information in the application and any supplemental documentation. In the event that USCIS approves the I-129, it approves the issuance of an H-1B visa to the foreign beneficiary named in the application, following which the beneficiary may either pick up their visa at an American consulate (if they reside in a foreign country) or may have the visa mailed to them (if they reside in the United States).

12. Some petitioning employers, such as the SUBJECT COMPANIES, are in the business of applying for H-1B visas for employees who ultimately will be assigned to projects for a client of the petitioner's (an "end client"). The petitioning employer acts as an intermediary, by servicing its clients' need for labor to perform specified projects. In such visa applications, the petitioning employer demonstrates that the proposed foreign-

---

[4] For instance, the I-129 requires the petitioner to "certify under penalty of perjury that this petition and the evidence submitted with it are true and correct to the best of my knowledge." In the accompanying instructions for the I-129, the Petitioner is advised that "[b]y signing this form, you have stated under penalty of perjury (28 U.S.C. section 1746) that all information and documentation submitted with this form is true and correct." The instructions also add that "[i]f you knowingly and willfully falsify or conceal a material fact or submit a false document with your Form I-129, we will deny your Form I-129 and any other immigration benefit. . . . In addition, you will face severe penalties provided by law and may be subject to criminal prosecution." Thus, when a petitioner signs the Form I-129, it assumes the legal responsibility for the truth and accuracy of all information submitted. If an I-129 is not signed, it will not be considered properly filed.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

national beneficiary will be assigned to an end-client project that qualifies as a "specialty occupation" by submitting proof of its commercial relationship with the end client and proof that the foreign-national beneficiary will work on a project for the end client.

13. More specifically, in my experience and training, petitioning employers that seek H-1B visas for employees who will be assigned to the petitioner's end clients typically will submit the following types of documents[5]:

a. **End-client letters** are letters submitted by the petitioner's end client or the third party worksite at which the foreign-national employee will work.[6] The letter generally certifies that the end client has agreed with the petitioning employer that the foreign-national employee will work on a specialty occupation for the end client. In my experience, such letters set forth the name of the foreign-national employee, their future job title, the project(s) to which they will be assigned to, the name of their onsite supervisor, and the projected duration of the foreign-national employee's services for the end client.

b. **Master Service Agreements** ("MSA") between the petitioner, vendor (if any), and the end client are used to clarify and establish the business/contractual relationship(s) between the parties.

c. **Statements of Work** ("SOWs") are contracts between the petitioner, vendor (if any), and end client, and generally serve as contractual extensions to the MSA. SOWs are generally used to specify in greater detail the terms of the end client's project and are sometimes referred to as "Purchase Orders."

---

[5] At all times relevant to the investigation, USCIS has published instructions regarding petitions for nonimmigrant workers. The USCIS instructions direct petitioning employers to include with their petitions "evidence" to support the statements made in petitions, including evidence of the foreign national's educational background, a copy of the employment agreement between the foreign national and the petitioning employer, and evidence regarding the purported client projects to which the foreign national purportedly will be assigned.

[6] Certain end clients use so-called "trusted vendors" to coordinate their labor needs. In such cases, the "end-client letter" will be submitted by one of those "trusted vendors" and will contain all of the information that an end-client letter generally includes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. **Company-support letters** are written by the petitioning company to USCIS on behalf of the foreign worker and identify the foreign worker by name, job duties, education and skills, and establish the contractual relationship(s) between the end client, vendor and any subcontractors.

14. Though USCIS does not require petitioning employers to submit such supporting documentation with their applications, in my experience, the absence of such documentation typically will result in USCIS issuing a Request for Evidence ("RFE") to the petitioning employer. Because an RFE can significantly delay the adjudication and issuance of an H-1B visa, petitioning employers ordinarily seek to submit as much supporting documentation as possible with their initial visa applications. Moreover, in the event that USCIS issues an RFE seeking additional evidence regarding a purported client project described in the petition, petitioning employers may submit these types of documents in order to prove the existence of that project and to prove that the foreign national will be assigned to it.

15. The validity date for an H-1B visa is determined by USCIS based on the petitioner's stated dates of employment for the foreign worker/beneficiary, as well as the evidence submitted in support of the petition. The maximum initial issuance period for an H-1B visa is three years, but can be extended for an additional three years, for a total of six years. In the event that the beneficiary's employment concludes prior to the visa's expiration date, the visa typically can continue to be used by the beneficiary for subsequent employment, so long as notification of the change is made to USCIS and DOL.

16. Even if the petitioner acts on behalf of an end client, unless and until the beneficiary's visa has expired or has been transferred to a new petitioning company, the petitioner is the formal employer of the beneficiary. While working at or for the end client, the employee is paid by the petitioner, and it is standard industry practice that the petitioner is paid an ongoing fee by the end client that covers the cost of the wage or salary as well as a profit margin for the petitioner.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. *Background Regarding "Bench-and-Switch" Visa-Fraud Schemes*

17. In my training and experience, the H-1B application process sometimes is used to perpetuate fraud, including through the use of false statements in application materials. Petitioning employers typically engage in such schemes in order to gain an unfair competitive advantage in the labor market.

18. I have investigated numerous fraud schemes that commonly are referred to as "bench-and-switch" schemes. In a "bench-and-switch" scheme, a petitioning employer falsely claims to USCIS that a foreign-national beneficiary already has been assigned to a project at an end client of the petitioner's. The fraudulent application includes documents that purports to substantiate the foreign-national beneficiary's job assignment at the end client.

19. In reality, the foreign national has not been assigned to work for any such end client, and the purported documents submitted in support of the claim are false and/or doctored. In some cases, the purported end client is a fictitious company that the petitioning employer has created (and, sometimes, conspired with others to create) in order to perpetuate the fraud.

20. In successful "bench-and-switch" schemes, petitioning employers obtain H-1B visas for foreign-national employees through false representations to USCIS. Once those visas are granted, or even before the visas are formally approved, the petitioning employer markets the foreign national to end clients other than those named in the actual petition. By doing so, the petitioning employer can shorten (or eliminate entirely) the ordinary lag time between when an end client agrees to use a foreign-national employee and when DHS issues an H-1B visa to that employee. Shortening or eliminating the lag time enables petitioning companies to place employees at end clients faster than their competitors are able to.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IV. FACTS ESTABLISHING PROBABLE CAUSE

21. On or about November 19, 2015, I was assigned to investigate the SUBJECT COMPANIES due to suspected visa fraud. Specifically, during its review of certain I-129 petitions filed by the SUBJECT COMPANIES, USCIS developed reason to believe that the SUBJECT COMPANIES had filed petitions claiming that the foreign nationals named in the petitions would be working on particular client projects that did not actually exist. Since opening my investigation, I have reviewed the SUBJECT COMPANIES' filed petitions (including supporting materials) from 2011 to the present, interviewed several former and current employees and contractors at the SUBJECT COMPANIES, reviewed email records, reviewed records produced by the SUBJECT COMPANIES' actual clients, and reviewed records produced by the purported clients named in the petitions. Based on those investigative steps, I have developed probable cause to believe all of the following, which is discussed in further detail in the subsections below:

a. ***First***, I have developed probable cause to believe that petitions filed by the SUBJECT COMPANIES between 2012 and 2015 contained false statements and forged documents.[7]

b. ***Second***, I have developed probable cause to believe that SAMAL knew about, and indeed helped prepare, the false statements and forged documents in the SUBJECT COMPANIES' petitions.

c. ***Third***, I have developed probable cause to believe that SAMAL knew that the statements in the petitions were false and that the documents attached to the petitions were fraudulent and forged.

---

[7] To be clear, my reference to petitions filed between 2012 and 2015 is not meant to imply that petitions filed outside of that timeframe were accurate. The Government is continuing to investigate petitions filed by the SUBJECT COMPANIES *after* 2015, including petitions filed in 2016 and 2017. Because this affidavit is being submitted for the purpose of establishing probable cause that SAMAL committed the offense set out in Count One, I do not discuss the Government's findings with regard to the post-2015 petitions.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. *Between 2012 and 2015, the SUBJECT COMPANIES Filed False and Fraudulent Petitions for Nonimmigrant Workers*

22. Between 2012 and 2015, Divensi filed approximately seventy-one (71) petitions for nonimmigrant workers in which it claimed that the foreign national named in each petition already had been designated to work at Divensi's offices on a project for a corporate end-client named referred to herein as CLIENT A. During the same timeframe, Azimetry filed approximately sixty-six (66) petitions for nonimmigrant workers in which it claimed that the foreign national named in each petition already had been designated to work at Azimetry's offices on a project for a corporate end-client referred to herein as CLIENT B. The petitions include the petition that is the subject of Count One: an April 24, 2014 Petition for Nonimmigrant Worker filed by Azimetry for a foreign-national referred to herein as "L.N.," in which Azimetry claimed that L.N. would be assigned to a project for CLIENT B. USCIS approved the petition on September 11, 2014.

23. To assert that the foreign nationals named in the petitions would be assigned to projects for CLIENT A and CLIENT B, the SUBJECT COMPANIES made the following statements in, and attached the following documents to, their petitions:

a. In cover letters to petitions, Divensi claimed that the foreign nationals named in the petitions would be assigned to projects for CLIENT A. Azimetry's cover letters to its petitions likewise claimed that the foreign nationals named in the petitions would be assigned to projects for CLIENT B. The cover letters further claimed that the projects had a duration of three years – i.e., the maximum validity period for an H-1B visa.

b. In the I-129 forms, the SUBJECT COMPANIES claimed that the foreign nationals would work at the offices of the petitioning employer (i.e., Divensi or Azimetry) in Bellevue, Washington.

c. Divensi attached to its petitions purported contracts with CLIENT A and Azimetry attached to its petitions purported contracts with CLIENT B. Each contract, or so-called "Statement of Work" or "SOW," purported to describe a project

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that CLIENT B had retained Azimetry to perform or that CLIENT A had retained Divensi to perform. The project descriptions in the SOW matched the descriptions of the purported projects that appeared in the cover letters to the petitions.

d. The SUBJECT COMPANIES also attached to the petitions purported end-client letters that appeared to have been issued by CLIENT A (in the case of Divensi's petitions) or CLIENT B (in the case of Azimetry's petitions). The letters appeared on the issuing client's letterhead. CLIENT A's letters appeared to have been signed by CLIENT A's current CEO, V.K.,[8] and CLIENT B's letters appeared to have been signed by CLIENT B's director of production operations, R.M. The letters claimed that the foreign national named in the petition indeed had been assigned to a project for the client that issued the letter.

24. For instance, Azimetry's petition relating to "L.N." – the subject of Count One – attached a letter on CLIENT B's letterhead, which purported to have been addressed to USCIS and signed by R.M. The letter purported to "verify that [CLIENT B] will be using the services of [L.N.], an employee of Azimetry Inc., through our contract agreement with Azimetry." The letter further represented that [L.N.] will be providing services as a Network and Computer Systems Administrator." As CLIENT B's representatives have explained, the company did not issue the letter or authorize Azimetry to submit the letter on its behalf.

25. These statements and documents were material to USCIS' decision whether to approve each petition. The statements and documents were material because they attested to USCIS that the foreign nationals indeed had roles in "specialty occupation" fields, as the H-1B visa requires. The statements and documents also were material because they provided USCIS with information regarding the requested validity period of the visa and the project location.

[8] CLIENT A's current CEO was previously a managing director at his company. Earlier drafts of the fraudulent letters therefore referred to him by the title of Managing Director.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

26. The following facts establish probable cause to believe that the petitions' claims about the projects for CLIENT A and CLIENT B were false, and that the documents submitted in support of those projects were fraudulent and forged:

a. On January 18, 2018, CLIENT A's current CEO, "V.K.," whose signature appeared on the end-client letters that Divensi attached to its H-1B petitions, told me that he did not sign the end-client letters.[9] CLIENT A also produced records showing that Divensi never billed CLIENT A for the services of the foreign-national employees whose petitions, which Divensi submitted to USCIS between 2012 and 2015, claimed they would be working on a CLIENT A project.

b. On April 6, 2015, a representative of CLIENT B informed USCIS over email that CLIENT B did not issue the CLIENT B end-client letters, and did not agree to assign the foreign-national employees named in the underlying petitions to its projects. CLIENT B also produced records showing that Azimetry did not bill CLIENT B for any of the foreign-national employees whose petitions claimed they would be working on an Azimetry project. In particular, Azimetry did not bill CLIENT B for any work done by L.N., the foreign national named in the petition that is the subject of Count One, and L.N. never worked on any projects for CLIENT B.

c. I have interviewed fourteen foreign nationals who were named in the petitions submitted by Divensi and Azimetry, including L.N. (as discussed below). Those foreign nationals told me that they did not work on the projects described in their petitions and did not believe they would be assigned to any such projects.

d. The SUBJECT COMPANIES' internal email records, particularly their emails with the foreign nationals named in the petitions and with actual end clients also show that the statements and documents in the petitions were fraudulent.

---

[9] USCIS officers first emailed CLIENT A in or around March 2015, inquiring about the legitimacy of the end-client letters that Divensi had attached to its petitions. At that time, CLIENT A's representatives told USCIS that CLIENT A had not issued the end-client letters and never agreed to use the foreign-national employees named in those letters on its projects. CLIENT A has also produced an email that V.K. sent SAMAL in March 2015 regarding the USCIS inquiry, in which V.K. said "I received this email from the Visa office asking if I signed this. I did not. I don't even know who this resource is. This is concerning? Pls advise on how this happened?"

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Specifically, in numerous emails sent before petitions were filed and while petitions were pending adjudication by USCIS, the SUBJECT COMPANIES' employees told foreign-national employees that the companies planned to send the employees' resumes to clients other than CLIENT A and CLIENT B.

27. Email records and other evidence relating to L.N., the foreign national who was the subject of the petition referred to in Count One, make clear that the petition's representations about L.N. were false. For instance, even though the petition claimed that L.N. would be assigned to a project for CLIENT B, L.N. emailed three employees at the SUBJECT COMPANIES just weeks after the petition was filed (and while it was still pending adjudication) and stated: "I remember you telling me that I should look for jobs and let you know regarding the same so that you could put forward my resume to those openings." After the petition was approved, L.N. emailed the SUBJECT COMPANIES' employees on numerous occasions about the status of his job search. L.N. has since told me during a voluntary interview on January 31, 2017 that he did not have a project when his petition was filed, while his petition was pending, or even when he arrived in the United States. L.N. has also acknowledged that the statements in his petition about his purported project at CLIENT B were false.[10]

B. SAMAL Prepared the SUBJECT COMPANIES' Fraudulent Petitions

28. I have also developed probable cause to believe that SAMAL prepared the SUBJECT COMPANIES' fraudulent petitions, including the false statements and forged documents in those petitions claiming that the relevant foreign nationals would be assigned to projects for CLIENT A and CLIENT B. My belief is based on the facts set out in the paragraphs below.

[10] During his interview, L.N. initially claimed that he believed he would be working on a project for CLIENT B. When confronted with emails in which he and the SUBJECT COMPANIES' employees discussed the need for him to find a project, L.N. admitted that he knew at the time the petition was filed that there was no actual position for him at CLIENT B or any other end client, and that he would need to find such a project in the event his petition was approved.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

29. ***First***, SAMAL's name and signature appear in the section at the end of each Divensi I-129 petition, in which a representative of the petitioning employer attests that the information in the petition is true and correct, under penalty of perjury. In addition to signing all of the Divensi petitions claiming that the foreign nationals named in the petitions would work on projects for CLIENT A, SAMAL also signed forty-three (43) Azimetry petitions claiming that the foreign nationals named in the petitions would work on projects for CLIENT B. In particular, SAMAL signed the Azimetry petition relating to foreign national "L.N.," which is the subject of Count One.

30. ***Second***, email records show that SAMAL regularly received drafts of the fraudulent petition materials from an outside contractor who prepared petition materials for the SUBJECT COMPANIES, and from a High Ranking Executive at the SUBJECT COMPANIES. SAMAL received the petition materials before the SUBJECT COMPANIES filed them with USCIS, so that he could review and approve their content, before signing them. Two representative examples of the many emails that SAMAL received with drafts of petition materials are as follows:

a. On March 19, 2014, an outside contractor emailed SAMAL with drafts of the petition materials for a foreign national referred to herein as "A.K.," who would be the subject of an Azimetry petition. The drafts included a letter that purported to have been issued by CLIENT B, which claimed that A.K. had been assigned to work on a project for CLIENT B.

b. On January 1, 2013, an outside contractor emailed SAMAL with drafts of the petition materials for a foreign national referred to herein as "R.A.," who would be the subject of a Divensi petition. The drafts included a letter that purported to have been issued by CLIENT A, which claimed that R.A. had been assigned to work on a project for CLIENT A.

31. ***Third***, email records also show that SAMAL prepared fraudulent petition materials before they were filed. In particular, I have found emails in which the outside contractor, the High Ranking Executive, and/or other employees at the SUBJECT

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

COMPANIES sent SAMAL unsigned drafts of fraudulent end-client letters and directed SAMAL to affix signatures to those letters. Representative examples of such emails include:

a. On January 3, 2013, the outside contractor emailed SAMAL an unsigned draft of a purported end-client letter from CLIENT A for a foreign national "R.A.," which purported to claim that "R.A." would be assigned to a project for CLIENT A. The email stated "Dear PK: Please provide me with signed [CLIENT A] letter." The copy of the letter that Divensi later sent USCIS included what appeared to be V.K.'s signature.

b. On February 27, 2013, the outside contractor emailed SAMAL an unsigned draft of a purported end-client letter from CLIENT A for a foreign national "M.M.," which purported to claim that "M.M." would be assigned to a project for CLIENT A. The email stated "Dear PK: Please provide a signed [CLIENT A] end-client letter and give it to [HIGH RANKING OFFICIAL]. Also I think page 4 of the SOW delivery date is incorrect. It should be September 15, 2014. Can you provide a longer term SOW."

c. On March 28, 2014, SAMAL emailed a Human Resources Employee at the SUBJECT COMPANIES and asked the employee to send him the client letter for a foreign national "M.J." SAMAL's email claimed he needed to "fix some mistake" in the draft of the client letter. In response, on March 29, 2014, the Human Resources Employee emailed SAMAL a purported end-client letter from CLIENT A for "M.J.," which purported to claim that "M.J." would be assigned to a project for CLIENT A.

C. *SAMAL Knew the Petition Materials Were Fraudulent*

32. Finally, there is probable cause to believe that SAMAL knew the petitions materials were fraudulent – that is, SAMAL knew that, contrary to the assertions in the petitions, the foreign nationals *had not* been assigned to projects for CLIENT A or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CLIENT B and the end-client letters *had not* been issued by those clients. The evidence that SAMAL knew the petition materials were fraudulent is as follows.

33. ***First***, email records show that SAMAL never intended for foreign nationals to work on projects for CLIENT A or CLIENT B in the event their petitions were approved. In emails, SAMAL directed the SUBJECT COMPANIES' employees to "market" foreign nationals named in petitions, as soon as those petitions were approved (and, in some cases, while those petitions were pending). At SAMAL's direction, the SUBJECT COMPANIES' employees proceeded to send the foreign nationals' resumes to actual end clients (and agents of those clients), in order to determine whether those clients were interested in hiring the foreign nationals to serve as contractors on part-time projects. In short, these emails establish that, contrary to the assertions in petitions that he signed, SAMAL knew and indeed directed that the foreign nationals named in petitions would not work on projects for CLIENT A or CLIENT B (because, as explained above, no such projects existed).

34. Representative examples of SAMAL's emails to the SUBJECT COMPANIES' employees include the following emails:

a. On July 8, 2013, SAMAL emailed four employees at the SUBJECT COMPANIES, whose roles included marketing foreign-national employees to clients for short-term projects. In his email, SAMAL attached the resumes for various foreign nationals, whose petitions recently had been approved by USCIS. SAMAL included the note: "[H]ere is our bench resume. Please market them immediately."

b. On September 13, 2013, SAMAL emailed five employees at the SUBJECT COMPANIES, whose roles included marketing foreign-national employees to clients for short-term projects. SAMAL attached to his email the resume for a foreign-national employee, whose petition included a fraudulent CLIENT B letter and had been approved by USCIS nine days earlier. In his email, SAMAL told the companies' employees to "start marketing him immediately."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

35. ***Second***, SAMAL participated in other email chains in which one or more participants recognized that the SUBJECT COMPANIES' petitions were fraudulent. For instance:

a. In a July 5, 2013 email, a foreign national whose petition was pending informed SAMAL that he had signed an employment agreement with Divensi, but that he recognized the agreement was for "*USCIS purpose*" insofar as it made representations to USCIS about his salary and role.

b. In numerous emails, such as an August 13, 2014 email, employees at the SUBJECT COMPANIES reported to SAMAL about their "bench" candidates – i.e., candidates whose visas had been approved but who still had not been placed at projects. Foreign nationals sent similar emails to SAMAL; for instance, in an October 31, 2013 email, a foreign national, whose petition included a fraudulent CLIENT B letter, told SAMAL that she had "been trying hard to get a client but still not getting an interview call."

c. SAMAL also received emails in which the SUBJECT COMPANIES' employees directed foreign nationals to make false statements at visa interviews with U.S. consulate officers.[11] For instance, on November 24, 2013, the High Ranking Executive forwarded SAMAL an email exchange in which the executive instructed a foreign national to tell U.S. consular officers that the foreign national would be working on "an internal development position and they customize the product to different customers. They said I will be customizing for [CLIENT A] as first project and I have to work in Divensi establishment not at the customer site." The High Ranking Executive proceeded to tell the foreign national that "let me know once [you're] done and ready to fly [so that] recruiters can arrange interviews."

---

[11] In my training and experience, I am aware that, even after USCIS approves an employer's petition for a nonimmigrant worker, the foreign national must submit to a consulate interview in the event that he or she is located overseas at the time the petition is approved. The consulate officer has the authority to issue (or to deny) a visa stamp, based on that interview.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

36. ***Third***, SAMAL has made false statements that evidence his consciousness of guilt. Specifically, on May 31, 2017, during an interview in the presence of his counsel, SAMAL told me that the SUBJECT COMPANIES' High Ranking Executive had inserted copies of the fraudulent end-client letters into petitions without SAMAL's knowledge. SAMAL claimed that the only fraudulent CLIENT A or CLIENT B end-client letters he had seen were letters that those clients alerted him to when USCIS began its investigation in March 2015. In truth and in fact, and as explained above, numerous emails show that SAMAL received and prepared end-client letters before those letters were attached to the SUBJECT COMPANIES' petitions.

V. CONCLUSION

Based on the above facts, I respectfully submit that there is probable cause to believe that, on or about April 1, 2014, in Bellevue, within the Western District of Washington and elsewhere, Pradyumna Samal did knowingly and intentionally commit visa fraud, in violation of Title 18, United States Code, Section 1546.

Richard Lin, Complainant
Special Agent, Department of State

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant committed the offense set forth in the Complaint.

Dated this 24 day of April, 2018.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970